Please type a plus sign (+) Inside this box ⊞

UTILITY PATENT APPLICATION TRANSMITTAL (Only for new nonprovisional applications under 37 C F R § 1 53(b))		
	Attorney Docket No.	101058-0042
	First Inventor or Application Identifier	Lih-Jyh Weng
	Title	RANDOMIZER SYSTEMS FOR PRODUCING MULTIPLE-SYMBOL RANDOMIZING SEQUENCES
	Express Mail Label No.	EL024698343US

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility application contents

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ *Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
2. ☒ Specification [Total Pages 14]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings *(if filed)*
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. ☒ Drawing(s) [Total Sheets 3]
4. Oath or Declaration [Total Pages]
a ☒ Newly executed (original copy)
b ☐ Copy from a prior application (37 C.F R § 1.63(d))
(for continuation/divisional with Box 17 completed)
[Note Box 5 below]
I. ☐ DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 C F R. §§ 1 63(d)(2) and 1 33(b)
5. ☐ Incorporation By Reference (*useable if Box 4b is checked*) The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered to be part of the disclosure of the accompanying application and is hereby incorporated by reference therein

6. ☐ Microfiche Computer Program (*Appendix*)
7. Nucleotide and/or Amino Acid Sequence Sequence Submission
((if applicable, all necessary)
a. ☐ Computer Readable Copy
b. ☐ Paper Copy (Identical to computer copy)
c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ☒ Assignment Papers (cover sheet & document(s))
9. ☐ 37 C.F.R.§3.73(b) Statement (*when there is an assignee*) ☐ Power of Attorney
10. ☐ English Translation Document (*if applicable*)
11. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503) (*Should be specifically itemized*)
14. ☐ *Small Entity Statement(s) (*(PTO/SB/09-12)* ☐ Statement filed in prior application, Status still proper and desired
15. ☐ Certified Copy of Priority Document(s) (*if foreign priority is claimed*)
16. ☐ Other:

*NOTE FOR ITEMS 1 & 14: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C. F. R. §1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C. F. R § 1.28).

17. If a CONTINUING APPLICATION, *check appropriate box and supply the requisite information below and in a preliminary amendment*:
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: /
Prior application Information: *Examiner* *Group/Art Unit*:

18. CORRESPONDENCE ADDRESS

☐ Customer Number or Bar Code Label (Insert Customer No. or Attach bar code label here) or ☒ Correspondence address below

Name	Robert A. Cesari				
Address	Cesari and McKenna 30 Rowes Wharf				
City	Boston	State	MA	Zip Code	02110
Country	U. S. A.	Telephone	(617) 951-2500	Fax	(617) 951-3927

Name (Print/Type)	Robert A. Cesari	Registration No. (Attorney/Agent)	38,381
Signature	Robert A. Cesari	Date	September 14, 1999

09/14/99 JC542 U.S. PTO 09/395845 09/14/99

PATENTS
101058-0042

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re The Application of: Lih-Jyh Weng	)	
Serial No.: not yet assigned	)	Examiner: not yet assigned
Filed: herewith	)	Art Unit: not yet assigned
For: RANDOMIZER SYSTEMS FOR PRODUCING MULTIPLE-SYMBOL RANDOMIZING SEQUENCES	)	

Cesari and McKenna, LLP
30 Rowes Wharf
Boston, MA 02110
September 14, 1999

EXPRESS-MAIL DEPOSIT

"Express Mail" Mailing-Label Number: MAILINGLABELNUMBER

The following papers are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 C.F.R. §1.10:

_X_ Patent Application (14 pages including 36 claims)
_X_ Oath or Declaration
_X_ Utility Patent Application Transmittal Letter
_X_ Informal Drawing (3 sheets)
_X_ Check No. 1776 for $40.00
_X_ Fee Transmittal Letter
_X_ Assignment With Recordation Form Cover Sheet
_X_ Check No. 1778 for $1048.00

UNITED STATES PATENT APPLICATION

of

Lih-Jyh Weng

for a

RANDOMIZER SYSTEMS FOR PRODUCING MULTIPLE-SYMBOL RANDOMIZING SEQUENCES

RANDOMIZER SYSTEMS FOR PRODUCING MULTIPLE-SYMBOL RANDOMIZING SEQUENCES

BACKGROUND OF THE INVENTION

A randomizer sequence is a long, non-repeating sequence of symbols or bits that combine with a code word in order to randomize the code word symbols. One reason to randomize the symbols of the code word is to eliminate repeated patterns of symbols, such as patterns of all zero symbols, that may not always be accurately demodulated. The code words of interest are error correction code words that are produced by encoding data in accordance with an error correction code (ECC) over a Galois Field GF(2^m). Over GF(2^m), the sequence and the code word are combined by XOR'ing.

Before decoding, the randomizer sequence is removed from the randomized code word by combining the same sequence with the code word. The ECC code word can then be decoded in a conventional manner and errors in the code word data symbols corrected, as appropriate.

Randomizer circuits for producing multiple-bit non-repeating sequences are known. One such circuit is a binary maximal length linear feedback shift register, such as an m-bit shift register that produces a random sequence up to 2^m-1 bits. The bit sequence, however, is not generally long enough to combine with all of the bits of the ECC code word. Accordingly, the 2^m-1 bit sequence, or pattern, must be used multiple times in the same code word, and the randomizing of the code word symbols may be adversely affected.

SUMMARY OF THE INVENTION

The invention is a system that operates in accordance with one or more multiplier constants that are primitive elements of GF(2^m) to produce multiple-symbol non-

repeating randomizer sequences that are long enough to combine with all the symbols of ECC code words that are encoded over $GF(2^m)$. The randomizer sequence is thus used once in a given code word.

The system may, without rewiring, produce a number of different multiple-symbol randomizer sequences, such that a key may be needed to select the particular sequence used with a given code word. Accordingly, the system can be used also to encrypt the ECC code word. Further, the multiplier constants may be selected such that each randomizer sequence produced by the system is separated from every valid ECC code word by a predetermined minimum distance, as discussed in more detail below. The system can thus be used to provide mis-synchronization detection.

More specifically, the system includes a circuit that is set up in accordance with a polynomial with at least one coefficient, or multiplier constant, that is a primitive element of $GF(2^m)$, and produces a non-repeating sequence that includes 2^m-1 or more m-bit symbols. The particular sequence produced by the circuit is determined by the primitive element selected as the multiplier constant and the selected initial state of one or more registers in the circuit. The initial state is selected such that at least one of the registers contains a non-zero element of $GF(2^m)$, and thus, 2^m-1 different sequences may be produced by, for example, selecting a different initial state for the given register. If the primitive multiplier constant is also selected from, for example, a set of "p" possible multiplier constants, the system produces $p*(2^m-1)$ different sequences. If additional ones of the initial register states and/or the multiplier constants are selectable, the system may produce even greater numbers of sequences. Accordingly, the system may be used to encrypt the ECC code word by associating the code word with a particular initial state and/or multiplier constant. An unauthorized user would then have to try many possible multiple-symbol sequences, in order to remove the randomizer sequence from the randomized code word and reproduce the ECC code word.

The inventive system provides benefits that are not provided by the known prior randomizer systems. These prior systems produce relatively short random sequences that must be repeated in the code word and are thus not appropriate for encryption of the entire code word. Further, the prior systems produce sequences that are not necessarily

optimized for mis-synchronization detection, that is, sequences that are not predetermined minimum distances away from the valid ECC code words. Accordingly, the known prior randomizing systems do not provide as robust mis-synchronization detection

BRIEF DESCRIPTION OF THE DRAWINGS

The invention description below refers to the accompanying drawings, of which:

Fig. 1 is a functional block diagram of an encoding system constructed in accordance with the invention;

Fig. 2 is a functional block diagram of a decoding system constructed in accordance with the invention;

Fig. 3 is a more detailed functional block diagram of a randomizer circuit included in the systems of Figs. 1 and 2;

Fig. 4 is a functional block diagram of an alternative randomizer circuit; and

Figs. 5 and 6 are functional block diagrams of further randomizer circuits.

DETAILED DESCRIPTION OF AN ILLUSTRATIVE EMBODIMENT

Referring to Fig. 1, an encoder 2 encodes data in a known manner in accordance with a BCH code, for example, a distance d Reed-Solomon code over GF(2^m), to produce an ECC code word. At the same time a randomizer circuit 10 produces a multiple-symbol, non-repeating randomizer sequence. The symbols of the randomizer sequence are XOR'd to the corresponding symbols of the ECC code word in XOR gates 4, to produce a randomized code word for recording or transmitting.

Referring now to Fig. 2, when the randomized code word is later retrieved or received, a decoder 8 removes the randomizer sequence from the code word in XOR gates 4, before the code word is decoded by a conventional decoding subsystem 6. Accordingly, the randomizer circuit 10 used for decoding must generate the same randomizer sequence produced by the encoder 2 (Fig. 1). If necessary, the decoder 8 uses information in a key 9 to set the randomizer circuit 10 to the appropriate initial state, as discussed below. The key 9 is provided to the decoder 8 in a conventional manner.

Referring now to Fig. 3, a randomizer circuit 10 that is set up in accordance with a degree-one polynomial includes a multiplier 12, and a register 14 that is initially set to a non-zero element of $GF(2^m)$. The randomizer circuit depicted in the drawing generates a multiple-symbol randomizer sequence using the polynomial $x+\alpha^k$, where α^k is a primitive element of $GF(2^m)$. The sequence produced by the circuit is:

$$S_k = R\alpha^k, R(\alpha^k)^2, R(\alpha^k)^3 \ldots R(\alpha^k)^i$$

which is non-repeating for $i \leq 2^m-1$. By selecting R as different ones of the 2^m-1 non-zero symbols of $GF(2^m)$, the system may produce 2^m-1 different, non-repeating randomizer sequences, with each sequence including up to 2^m-1 m-bit symbols. The system may store particular values for R or may generate them by, for example, raising α to a selected power.

The system must use the selected value of R to reproduce the same sequence for decoding. As appropriate, the key 9 specifies or points to the selected value of R or, for example, the selected power to which α is raised to produce R.

For more robust encryption, the particular multiplier constant used to produce the randomizer sequence for a given code word may be selected from a set of "p" values. A general purpose multiplier (not shown) may then be used in the circuit 10 in place of the constant multiplier 12. Alternatively, as depicted in Fig. 4, p multipliers 12 may be included in the circuit, with a switch 16 selecting the particular multiplier to be used to produce the randomizer sequence for a given code word. The key supplied to the decoder must then include information that specifies both R and α^k. If the key is not provided, a user must test a possible $p*(2^m-1)$ sequences in order to remove the randomizer sequence from the randomized code word.

To provide mis-synchronization detection, the multiplier constant α^k may be selected to produce a randomizer sequence S_k that is a predetermined minimum distance away from every code word of the distance d Reed-Solomon code such that a mis-synchronized error results in a decoded code word that contains more errors than the ECC can correct .

As discussed above, the multiplier constant may be selected from a set of p values. For mis-synchronization detection, the values in the set must each produce sequences that satisfy the predetermined minimum distance requirements. Generally, if α^k produces a randomizer sequence that meets the predetermined minimum distance requirements, α^{2k}, α^{4k}, α^{8k}, ... $\alpha^{2^m k}$ also produces such a randomizer sequence. Accordingly, the p multiplier constants can be determined from $\frac{p}{m}$ tested values of α^k.

Referring now to Fig. 5, circuits that use polynomials with degrees greater than one may also be used to produce longer multiple-symbol, non-repeating randomizer sequences. The higher-degree randomizer circuits produce sequences of up to $(2^m)^y$-1 symbols, where y is the degree of the polynomial. These circuits may thus be used in systems in which the ECC is a primitive BCH code of degree y.

The drawing depicts a randomizer circuit 100 that is set up in accordance with a degree-two polynomial. The randomizer circuit 100 shown in the drawing includes two multipliers 102_1 and 102_2 and produces the randomizer sequence in accordance with the polynomial $x^2+\beta x+\gamma$, where β and γ are primitive elements of $GF(2^m)$. For any pair of primitive elements β and γ the randomizer sequence produced by the randomizer circuit 100 is specified by R_1 and R_2, which may be, respectively, any elements of $GF(2^m)$, where at least one of R_1 and R_2 is non-zero. There are thus many more possibilities for the randomizer sequences with this system since the values of β, γ, R_1 and R_2 may each be selected and the randomizer circuit 100 may thus provide more robust encryption than the system depicted in Fig. 1. The key that is supplied for decoding must specify the selected values, so that randomizer system can be set to the appropriate initial state to reproduce the randomizing sequence.

For mis-synchronization detection, the values of the multiplier constants and at least one of the values for the register are preferably selected together, to ensure that associate randomizer sequence satisfies the predetermined minimum distance requirements. For each selection, there are 2^m-1 possibilities for the associated value of the remaining register, and thus, 2^m-1 possible sequences.

Fig. 6 depicts an alternative degree-two randomizer circuit 110. Again, the circuit produces multiple-symbol randomizer sequences for selected values of β,γ, R_1 and/or R_2.

The foregoing description has been limited to specific embodiments of this invention. It will be apparent, however, that variations and modifications may be made to the invention, with the attainment of some or all of its advantages. Therefore, it is the object of the appended claims to cover all such variations and modifications as come within the true spirit and scope of the invention.

What is claimed is:

CLAIMS

1. A system for producing multiple-symbol randomizer sequences over $GF(2^m)$, the system including:

A. a first register for supplying an initial state, the register holding a non-zero element of $GF(2^m)$;

B. a first multiplier for multiplying the contents of the register by a multiplier constant that is a primitive element of $GF(2^m)$; and

C. first feedback means for

i. supplying the products produced by the multiplier as the symbols of the randomizer sequence, and

ii. supplying the symbols of the randomizer sequence to update the first register.

2. The system of claim 1 further including:

D. one or more second registers for holding elements of $GF(2^m)$;

E. one or more second multipliers for multiplying the contents of the one or more second registers by one or more multiplier constants that are elements of $GF(2^m)$;

F. an adder for adding the products produced by the first and second multipliers and supplying the sum to the first feedback means; and

G. second feedback means to supplying the contents of the first register to update the second register.

3. The system of claim 1 further including a selection means for selecting the initial state of the first register in order to produce a randomizer sequence that provides for encryption.

4. The system of claim 2 further including a selection means a means for selecting an initial state for the first register and the one or more second registers.

5. The system of claim 1 further including encryption means for encrypting a code word, the encryption means including:

a. selection means for selecting an initial state for use in producing the randomizer sequence;

b. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, the means producing a randomized code word; and

c. means for producing a key associated with the selected the initial state.

6. The system of claim 5 further including a decrypting subsystem for using the key to reproduce the randomizer sequence and removing the randomizer sequence from the randomized code word to reproduce the ECC code word.

7. The system of claim 1 wherein the multiplier constant is selected to produce randomizer sequences that are each a predetermined minimum distance from code words of a given BCH code.

8. The system of claim 6 further including means for detecting mis-synchronization, the mis-synchronization detection means including:

a. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, the means producing a randomized code word;

b. means for removing the randomizer sequence from the randomized code word to reproduce the ECC code word; and

c. a decoder for decoding the reproduced ECC code word, the decoder detecting a mis-synchronization if the number of errors in the reproduced ECC code word is greater than the number of errors that can be corrected by the given BCH code.

9. The system of claim 7 wherein the multiplier constant is further selected from a set of multiplier constants which each produce randomizer sequences that are at least a predetermined minimum distance from code words of a given BCH code.

10. The system of claim 9 further including a means for providing a key to select the multiplier constant for a given randomizer sequence.

11. The system of claim 2 wherein the multiplier constants are selected to produce randomizer sequences that are each a predetermined minimum distance from code words of a given BCH code.

12. The system of claim 11 further including means for detecting mis-synchronization, the mis-synchronization detection means including:

a. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, the means producing a randomized code word;

b. means for removing the randomizer sequence from the randomized code word to reproduce the ECC code word; and

c. a decoder for decoding the reproduced ECC code word, the decoder detecting a mis-synchronization if the number of errors in the reproduced ECC code word is greater than the number of errors that can be corrected by the given BCH code.

13. The system of claim 12 wherein the multiplier constants are further selected from a set of multiplier constants that produce randomizer sequences that are at least a predetermined minimum distance from code words of a given BCH code.

14. The system of claim 13 further including a means for providing a key to select the multiplier constants for a given the randomizer sequence.

15. The system of claim 1 further including

D. one or more second registers for holding elements of $GF(2^m)$;

E. one or more second multipliers for multiplying the contents of the first register by associated elements of $GF(2^m)$ and supplying the products to update the one or more second registers; and

F. one or more adders for adding the contents of the one or more second registers to the product produced by the first multiplier to produce a sum and supplying the sum to the first feedback means.

16. The system of claim 1 further including:

D. a plurality of second multipliers each for multiplying the contents of the register by a multiplier constant that is a primitive element of $GF(2^m)$; and

E. a switch for selecting one of the plurality of second multipliers or the first multiplier to produce the randomizer sequence.

17. The system of claim 16 further including encryption means for encrypting a code word, the encryption means including:

d. selection means for selecting an initial state for use in producing the randomizer sequence;

e. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, the means producing a randomized code word; and

f. means for producing a key associated with the selected the initial state.

18. The system of claim 17 further including decryption means for using the key to reproduce the randomizer sequence and removing the randomizer sequence from the randomized code word to reproduce the ECC code word.

19. The system of claim 18 wherein the selection means further selects the multiplier constant from a set of multiplier constants.

20. The system of claim 15 further including encryption means for encrypting a code word, the encryption means including:

g. selection means for selecting an initial state for use in producing the randomizer sequence;

h. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, the means producing a randomized code word; and

i. means for producing a key associated with the selected the initial state.

21. The system of claim 20 further including decryption means for using the key to reproduce the randomizer sequence and removing the randomizer sequence from the randomized code word to reproduce the ECC code word.

22. The system of claim 20 wherein the selection means further selects the multiplier constant from a set of multiplier constants.

23. A method for producing multiple-symbol randomizer sequences, the method including the steps of:

A. supplying an initial state to a first register;

B. producing a first product by multiplying the contents of the first register by a multiplier constant that is a primitive element of $GF(2^m)$;

C. supplying the first product as

a. a next symbol of the randomizer sequence, and

b. an to update the first register;

D. repeating steps A-C i times for $i \leq 2^m-2$.

24. The method of claim 23 further including:

E.. in the step of supplying the initial state further including supplying an initial state to a second register;

F. in the step of producing a first product further including multiplying the contents of the second register by a multiplier constant that is an element of $GF(2^m)$ and adding the result to the first product; and

G. in the step of supplying the first product further including supplying the contents of the second register to update the first register.

25. The method of claim 23 further including the step of selecting the initial state for the first register in order to produce a randomizer sequence for encryption.

26. The method of claim 25 further including, in the step of selecting the initial state, selecting the initial state of the second register.

27. The method of claim 26 further including the step of associating with each randomizer sequence a key that indicates the associated selected initial state.

28. The method of claim 23 further including in the step of producing the fist product further including selecting the multiplier constant to produce randomizer sequences that are each a predetermined minimum distance from code words of a given BCH code.

29. The method of claim 28 further including the step of detecting mis-synchronization by

a. combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, to produce a randomized code word;

b. removing the randomizer sequence from the randomized code word to reproduce the ECC code word; and

c. decoding the reproduced ECC code word and detecting a mis-synchronization if the number of errors in the reproduced ECC code word is greater than the number of errors that can be corrected by the given BCH code.

30. The method of claim 28 wherein in the step of producing the first product further includes selecting the multiplier constant from a plurality of multiplier constants which each produce randomizer sequences that are respectively a predetermined minimum distance from code words of a given BCH code.

31. The method of claim 30 further including the step of providing a key to select the multiplier constants associated with a given randomizer sequence.

32. The method of claim 23 further including

E. in the step of supplying the initial state supplying the initial state of one or more second registers;

F. in the step of producing the first product including the step of multiplying the contents of the first register in one or more second multipliers by associated primitive elements of $GF(2^m)$ and supplying the products to update the one or more second registers; and

G. in the step supplying further including the step of adding the contents of the one or more second registers to the product associated with the contents of the first register and supplying the sum as the next sequence symbol and to update the first register.

33. The method of claim 23 further including in the step of producing the first product selecting a multiplier constant from a plurality of multiplier constants.

34. The method of claim 23 further including a step of encrypting a code word by:

j. selecting an initial state for use in producing the randomizer sequence;

k. combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$ to produce a randomized code word; and

l. producing a key associated with the selected the initial state.

35. The method of claim 34 further including a step of decrypting the code word by using the key to reproduce the randomizer sequence and removing the randomizer sequence from the randomized code word to reproduce the ECC code word.

36. The method of claim 34 wherein the step of selecting the initial state further includes selecting one or more multiplier constants.

ABSTRACT OF THE DISCLOSURE

A system that produces one or more non-repeating randomizer sequences of up to 2^m-1 or more m-bit symbols includes a randomizer circuit that is set up in accordance with a polynomial with primitive elements of GF(2^m) as coefficients. The system combines the randomizer sequence with all the symbols of ECC code words that are encoded using a BCH code over GF(2^m) to produce a randomized code word. The particular primitive elements used and/or an initial state of one or more registers in the system specifies the particular sequence produced by the system. The initial state of each of the one or more registers is a selected one of the 2^m-1 elements of GF(2^m), and thus, 2^m-1 different sequences may be produced by selecting a different initial state for a given one of the registers. If the coefficients are also selected from, for example, a set of "p" possible values, the system produces p*(2^m-1) different sequences. The system may thus be used to encrypt the ECC code word by associating the code word with a particular selected initial state and/or coefficient. The coefficients may be selected to produce randomizer sequences that are predetermined minimum distances away from both the ECC code words.

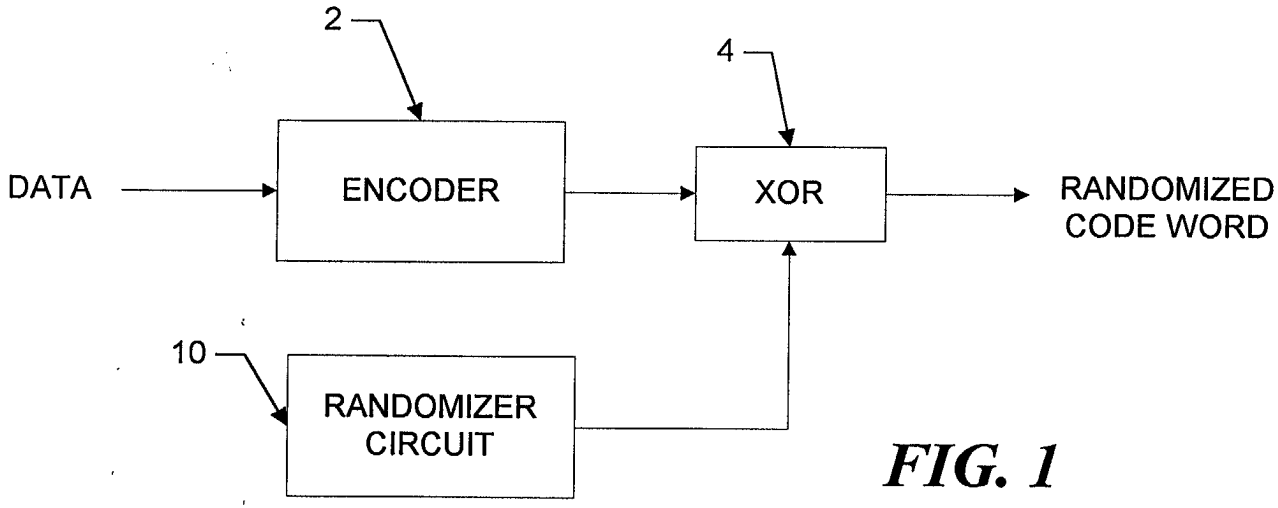

FIG. 1

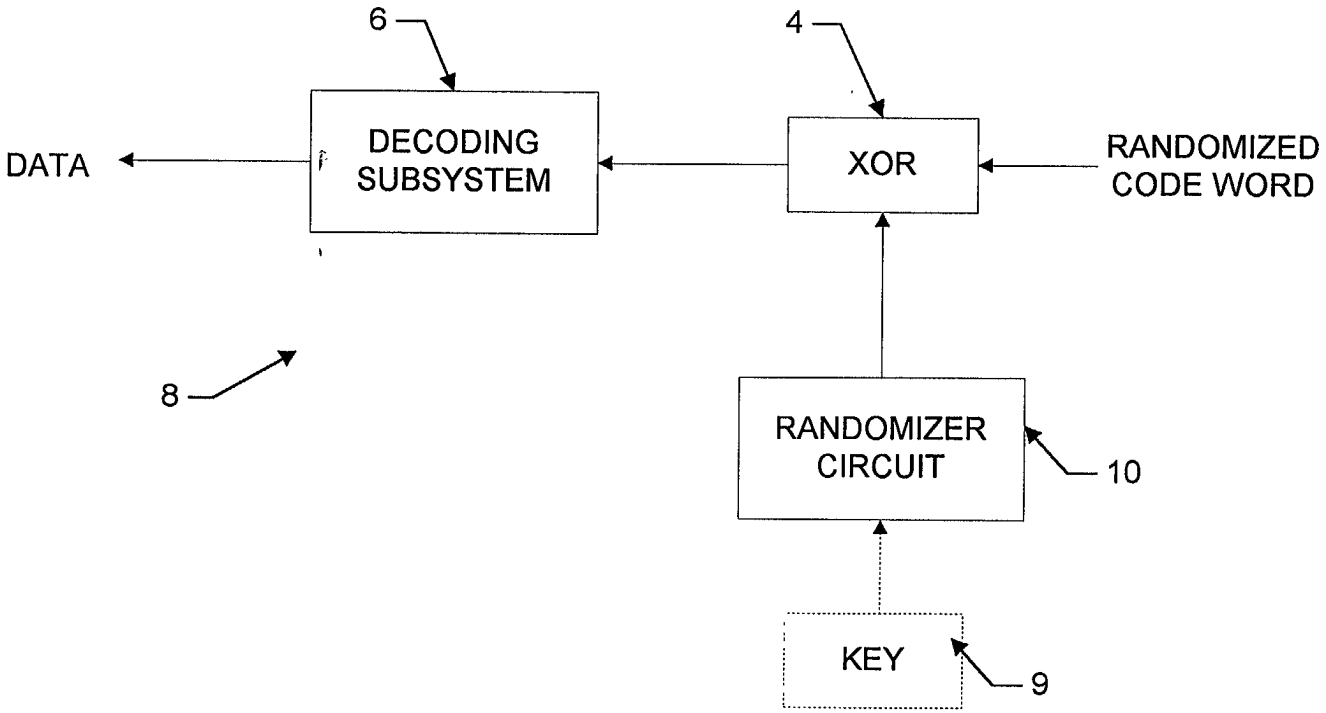

FIG. 2

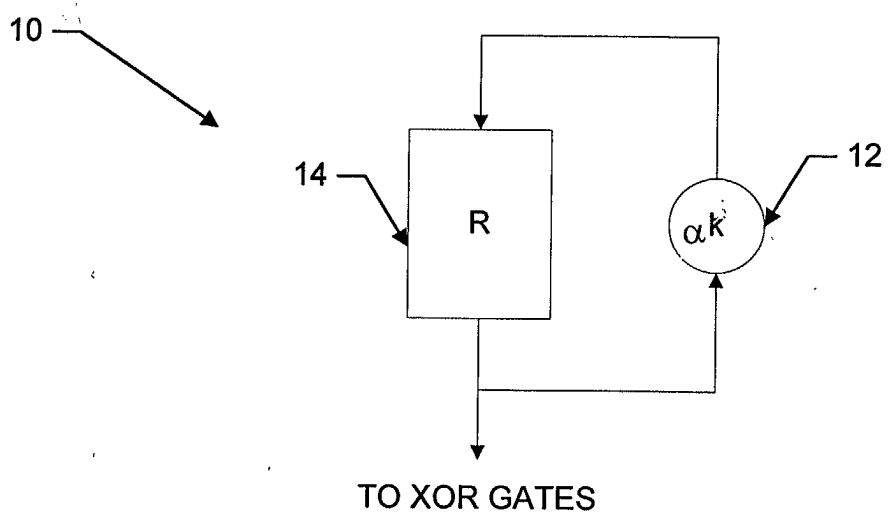
10
14
R
12
α^k
TO XOR GATES

FIG. 3

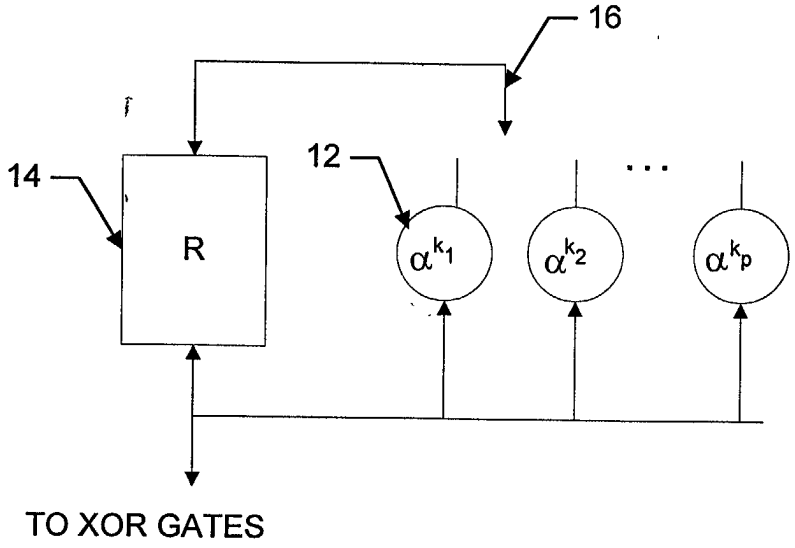
16
14
R
12
α^{k_1}
α^{k_2}
α^{k_p}
TO XOR GATES

FIG. 4

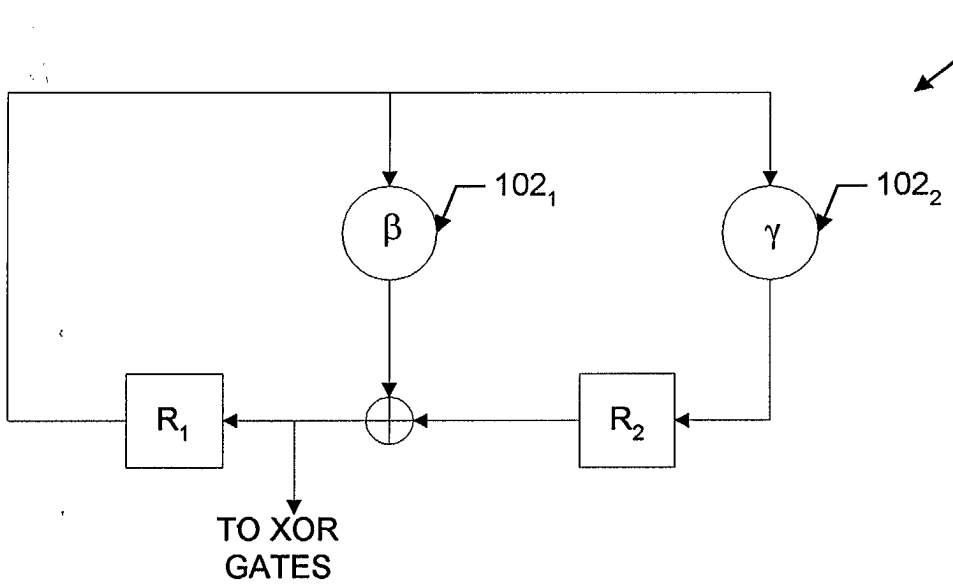

FIG. 5

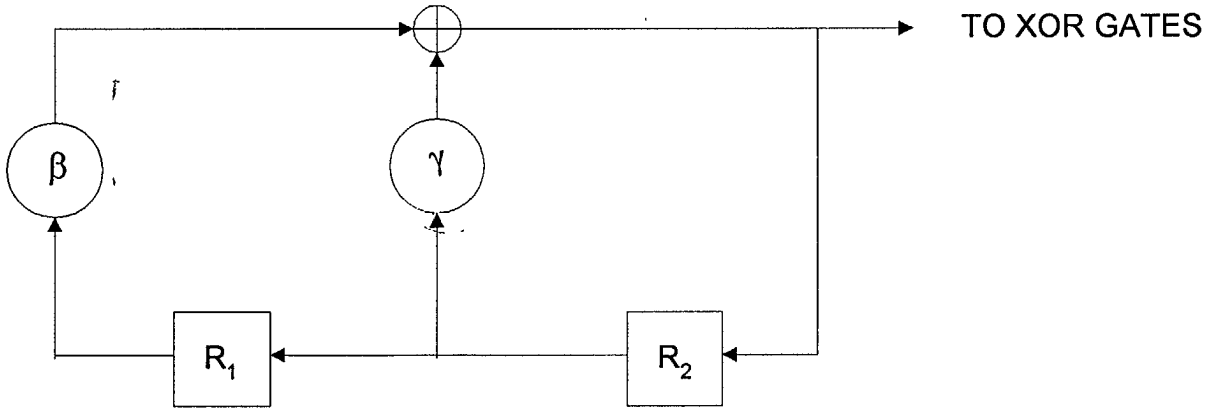

FIG. 6

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below-named inventor, I hereby declare that:

My residence, post-office address, and citizenship are as stated below next to my name.

I believe I am the original, first, and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled RANDOMIZER SYSTEMS FOR PRODUCING MULTIPLE-SYMBOL RANDOMIZING SEQUENCES, the specification of which is attached hereto and identified by Cesari and McKenna File No. 101058-0042.

I hereby state that I have reviewed and understand the contents of the above-identified application specification, including the claims, as amended by any amendment specifically referred to herein.

I acknowledge the duty to disclose all information known to me that is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code §119(a)-(d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate filed by me on the same subject matter having a filing date before that of the application on which priority is claimed: None.

I hereby claim the benefit under Title 35, United States Code §119(e) of the following U.S. provisional application: None.

I hereby claim the benefit under Title 35, United States Code §120, of the United States Application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United State Code, §112, I acknowledge the duty to disclose all information that is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56, and which became available to me between the filing date of the prior application and the national or PCT international filing date of this application: None.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint Michael E. Attaya, Reg. No. 31,731; Charles J. Barbas, Reg. No. 32,959; Joseph H. Born, Reg. No. 28,283; Robert A. Cesari, Reg. No. 18,381; Yong S. Choi, Reg. No. 43,324; Brian C. Dauphin, Reg. No. 40,983; Steven J. Frank, Reg. No. 33,497; Christopher K. Gagne, Reg. No. 36,142; A. Sidney Johnston, Reg. No. 29,548; William A. Loginov, Reg. No. 34,863; John F. McKenna, Reg. No. 20,912; Martin J. O'Donnell, Reg. No. 24,204; Thomas C. O'Konski, Reg. No. 26,320; Michael R. Reinemann, Reg. No. 38,280; Rita M. Rooney, Reg. No. 30,585; Heather B. Shapiro, Reg. No. 41,305; Patricia A. Sheehan, Reg. No. 32,301; and Joseph Stecewycz, Reg. No. 34,442, Cesari and McKenna, LLP, 30 Rowes Wharf, Boston, Mass. 02110, jointly, and each of them severally, my attorneys and attorney, with full power of substitution, delegation and revocation, to prosecute this application, to make alterations and amendments therein, to receive the patent and to transact all business in the Patent and Trademark Office connected therewith. Please direct all telephone calls to Patricia A. Sheehan at (617) 951-2500. Please address all correspondence to Patricia A. Sheehan.

Lih-Jyh Weng — Date: Sept 8, 1999

Residence: 95 Brookdale Circle
Shrewsbury, MA 01545

Citizenship: United States

Post Office Address: Same as above